Quantum key distribution system operating at sifted-key rate over 4 Mbit/s[1]

Xiao Tang[2], Lijun Ma, Alan Mink[3], Anastase Nakassis, Hai Xu, Barry Hershman, Joshua Bienfang,
David Su, Ronald F. Boisvert, Charles Clark, and Carl Williams
National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899

ABSTRACT

A complete fiber-based polarization encoding quantum key distribution (QKD) system based on the BB84 protocol has been developed at National Institute of Standard and Technology (NIST). The system can be operated at a sifted key rate of more than 4 Mbit/s over optical fiber of length 1 km and mean photon number 0.1. The quantum channel uses 850 nm photons from attenuated high speed VCSELs and the classical channel uses 1550 nm light from normal commercial coarse wavelength division multiplexing devices. Sifted-key rates and quantum error rates at different transmission rates are measured as a function of distance (fiber length). A polarization auto-compensation module has been developed and utilized to recover the polarization state and to compensate for temporal drift. An automatic timing alignment device has also been developed to quickly handle the initial configuration of quantum channels so that detection events fall into the correct timing window. These automated functions make the system more practical for integration into existing optical local area networks.

Keywords: Quantum key distribution, polarization auto-compensation, automatic timing alignment, BB84 protocol

1. INTRODUCTION

Since proposed by Bennett and Brassard in 1984 [1], quantum key distribution (QKD) has been studied extensively. QKD systems provide for the transmission of cryptographic key data whose security is guaranteed by the fundamental quantum properties of single photons [2]. QKD systems are operated either in free-space [3, 4] or over optical fiber [5-9]. At NIST, a QKD system based on the B92 [10] protocol with transmission over 1 km of optical fiber was developed in 2005 [5]. In that system, bits were encoded in photon polarization states. Since such states may evolve during transmission in fiber, manually adjusted polarization controllers were used to enable state recovery. The sifted key rate of the system was more than 1 Mbit/s for 1 km fiber and mean photon number 0.1.

To further increase the sifted-key rate and improve the security properties of the system, we recently converted the underlying QKD protocol from B92 to BB84 and increased quantum transmission rate from 312.5 to 625 Mbit/s. Now the system can run at a sifted-key rate over 4 Mbit/s with 1 km fiber and mean photon number 0.1 while realizing a quantum error rate is as low as 3.4%. This is, to our knowledge, the highest sifted-key rate with such low error rate ever reported. We have also developed a polarization auto-compensation module that traces the polarization temporal drift during the transmission in fiber and recovers polarization states. With the polarization auto-compensation module the system provides both high levels of stability and performance. Furthermore, an automatic timing alignment device has also been developed and utilized, which greatly eases the system initialization process. These additional features will allow us to demonstrate field operation of the system in the future.

[1] The identification of any commercial product or trade name does not imply endorsement or recommendation by the National Institute of Standards and Technology.

[2] xiao.tang@nist.gov; phone 301-975-2503; www.nist.gov

[3] alan.mink@nist.gov; phone 301-975-5681; www.nist.gov

Quantum Information and Computation IV, edited by Eric J. Donkor, Andrew R. Pirich, Howard E. Brandt,
Proc. of SPIE Vol. 6244, 62440P, (2006) · 0277-786X/06/$15 · doi: 10.1117/12.664455

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
2006

2. REPORT TYPE

3. DATES COVERED
00-00-2006 to 00-00-2006

4. TITLE AND SUBTITLE
Quantum key distribution system operating at sifted-key rate over 4 Mbit/s

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Institute of Standards and Technology,100 Bureau Dr,Gaithersburg,MD,20899

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	17. LIMITATION OF ABSTRACT **Same as Report (SAR)**	18. NUMBER OF PAGES **8**	19a. NAME OF RESPONSIBLE PERSON

In order to integrate the system into existing optical local area networks (LANs), we consider four possible options. Two of these, in which two fibers are used, were experimentally demonstrated in this work. It is also possible to utilize a single fiber for both quantum and classical channels, with additional losses being introduced. In practice the option selected would depend upon the condition of the existing LAN and user requirements.

In this paper, we describe the system configuration in Section 2, including the system structure, automatic polarization compensation module and automatic timing alignment. In Section 3 we present experimental results and discuss the system's performance. In Section 4, we also propose schemes for integrating the system into existing LANs.

2. SYSTEM CONFIGURATION

2.1 System structure

In this QKD system, cryptographic keys originate with a transmitter, Alice, and a receiver, Bob. Figure 1 illustrates the system's structure. Similar to our previous fiber-based QKD system with B92 [10], we use 850 nm photons in the quantum channel to meet the detection range of silicon-based avalanche photo diode (APD) and 1510 and 1590 nm in the bi-directional classical channels. The system operates at a synchronized clock rate of 1.25 Gbit/s, enabling a quantum channel transmittance rate (QCTR) as high as 625 Mbit/s (2 clock periods).

At the transmitter, four 10 Gbit/s 850 nm Vertical Cavity Surface Emitting Lasers (VCSELs) controlled by a high-speed data handling board in Alice's computer generate laser pulses. The intensity of the laser pulses are then attenuated by variable optical attenuators (VOA) to the single photon level. The polarization orientation of these photons in the four paths dictated by the BB84 protocol are set to -45º, +45 º, 0º and 90 º respectively by four linear polarizers and a half-wave plate (HWP). They are then combined into a non-polarizing beam-splitter (NPBS). The mean photon number (μ) at the output point of Alice is set to 0.1, i.e. on average, Alice emits one photon every ten pulses.

At the receiver, a 1 x 2 non-polarizing single-mode fiber coupler performs a random choice of polarization basis for encoding 0/1 bit values, either the horizontal/vertical (HV) basis or the -45º/+45 º (45 º) basis. After the coupler, a polarization auto-compensation module recovers the photon's polarization state. In each path, a polarizing beam-splitter (PBS) separates the photons by their polarization and leads them, through an interference filter (I.F.), to a corresponding APD. A photon entering into the correct detection basis is detected by a certain APD and its value will be considered valid during subsequent key-sifting, while a photon entering into an incorrect detection basis would be detected by each of the two APDs in the basis with 50% possibility and its value will later be discarded by key-sifting. The counts detected by each APD are routed to a high-speed data handling board in Bob's computer.

The pair of high-speed data handling boards, designed and implemented at NIST, communicating with Alice and Bob's computers via a PCI bus. The boards manage all aspects of high-speed data generation and processing needed to create a shared sifted key according to the BB84 protocol [11]. In particular, Alice's board generates a pseudo-random data stream to feed the quantum channel and a stream of synchronizing pulses on the classical channel, each at 1.25Gbit/s. Bob's board recovers and synchronizes the clock from the classical channel data stream and receives the detected photon signal from the APDs. Bob's board then sends the bit position and the measuring basis, but not the bit value, back to Alice over the classical channel. After matching each detection event with the corresponding event of the stored bit-stream, Alice tells Bob which detection events are valid (i.e., measuring basis matches encoding basis) via the same classical channel. At this point, Alice and Bob share a so-called "sifted key". Alice and Bob then send the sifted bit values to their own computers for subsequent error reconciliation and privacy amplification necessary to generate shared secret keys [12]. The sifted-key rate and the quantum bit error rate (QBER), two important metrics for QKD systems, can be measured in real time from the raw data before reconciliation in the system. With the BB84 protocol, the system provides better security property than the previous B92 version [13].

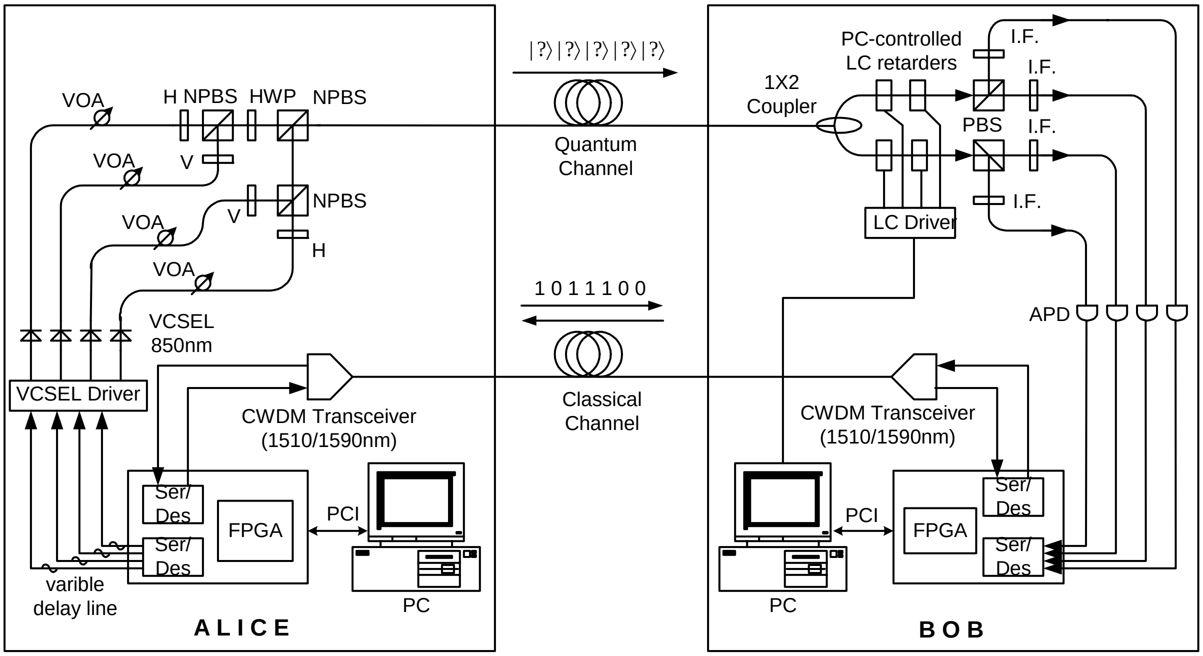

Figure 1. Experimental setup

2.2 Polarization recovery and compensation

For a fiber-based QKD system with polarization encoding, polarization recovery must be implemented. In our previous B92 system, we used two manual polarization controllers for a laboratory demonstration. In this newer BB84 based system, we have developed a polarization auto-compensation module that allows for quicker and easier initializing the system and stabilizing the performance automatically.

The polarization auto-compensation (PAC) module consists of two identical actuators that control the polarization state in each detection basis. Each actuator is formed by two liquid crystal retarders (LCR). The axis of each LCR is pre-aligned with the polarizing beam splitter (PBS) (Fig. 2) and its relative phase retardance is controlled by a computer. It can be proved that with proper applied voltages and hence, the phase retardance of LCRs, the BB84 protocol can be realized. In a PAC procedure, by turning on/off relevant VCSELs, and based on the feedback from the output of the corresponding APDs, the computer can automatically search for proper retardance of each LCR and then hold it for optimal performance in accordance with the BB84 protocol. To enable long-term operation, the QKD system periodically suspends quantum bit transmission and the PAC traces and compensates the polarization evolution in the quantum channel.

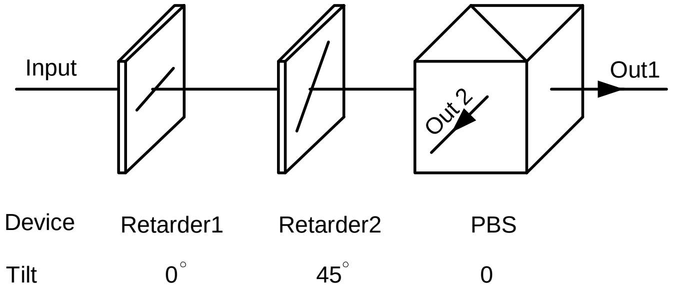

Figure 2. Retardance of the LCRs and their alignment related to the PBS

In our experiment, for both paths at Bob, if the photons arrive at the correct measuring basis we are able to obtain over 20 dB of extinction ratio, the ratio of the counts from the two APDs in the basis. If the photons arrive at incorrect measuring basis, we will obtain nearly equal counts from the two APDs in the basis. The PAC has been tested in the laboratory environment. With the polarization auto-compensation module running every 15 minutes, the extinction ratio in the correct measuring basis is kept above 21 dB for 24 hours in the experiment.

The PAC procedure operates in two modes, the initialization mode and the tracking mode. The initialization mode conducts a complete search over the entire state space to find the optimal LCR setting. In the tracking mode PAC begins its search from the last known optimal operating point assuming that small drifts from that point have occurred. A fiber-based QKD system in the field will experience polarization drifts more quickly and significantly than that in the laboratory, and therefore, PAC operation time of tracking mode becomes a critical issue. The operation time of tracking mode is mainly determined by three factors: (1) time for collecting enough photon counts to form a sufficient feedback signal (about 50 ms in our case); (2) response time of the LCR (100 ms according to the specifications [14]); and (3) how far the polarization has drifted from the previous optimal point, which dependents on environmental conditions. We have designed a searching protocol for tracking mode to reach the optimal point. In the protocol, it needs 9 sampling points to finish one step and the number of steps is dependent on the polarization drift during the time interval between PAC operations. In our laboratory environment, the PAC tracking operation time is from 1.2 to several seconds in each operation when the PAC takes action every 15 minutes. For further development, we will choose faster polarization controllers to reduce response time. In addition, data rate and mean photon number will be increased during PAC operation for a shorter collecting time. Also the interval time between two PAC actions will be modified according to environmental conditions.

2.3 Time alignment

In the quantum channel, there are four separate paths in Alice and Bob, though they all share a common fiber during quantum bit transmission between them. Therefore, the photons may have somewhat different propagations time in these paths. In addition, the large losses in the quantum channels result in detection events being unsynchronized, sparse and random. In a synchronized high speed QKD system aligning detection events to a specific narrow time window is critical. In our system the clock signal is generated through the classical channel. The timing alignment procedure includes four steps. First, synchronization between the classical channel and all four optical paths in the quantum channel must be established. Second, an electrical variable delay line is utilized in the signal feeding cable for each VCSELs. The four variable delay lines are aligned during system setup to guarantee the same time delay from the moment when Alice sends a trigger signal to the moment when the photon arrives at the NPBS right before insertion into the common fiber. In our implementation we purposely used the same fiber length for each optical path so that a photon from any of the four VCSELs takes the same optical transmission time to arrive at any of four APDs. In step three, an electrical delay chip on Bob's board is used to output signals from each of four APDs. These delay chips can be adjusted automatically (0.8 ns/step) to ensure that the output signal from each APD takes roughly the same electrical transmission time to arrive at the comparison point with the clock. In step four, a fine timing delay adjustment (40 ps/step) is utilized in each of four electrical paths on the board to provide an accurate bit position shift within the time window. This fine adjustment enables the system to keep most of the corresponding quantum bits in the same time window, resulting in a reduction of the error rate.

An automated procedure has been designed, which aligns the paths in the quantum channel with the classical channel by computing the delays in quantum paths. This procedure is part of the startup configuration process, once configured the delays don't change. This procedure continuously sends a known quantum data stream and uses that information to first set the values of the sub-bit timing, programmable delay chips on Bob's data handing board. Then it determines the bit delay values for each of the quantum paths and sets that value on Bob's data handing board. The manual procedure took about a half hour to an hour. This automated procedure takes about minutes and could be sped up more if desired

3. EXPERIMENTAL RESULTS AND DISCUSSION

In a high speed QKD system, the sifted-key rate *R* can be estimated by the following equation if the influence of the APD's dead time is ignored:

$$R = \mu \cdot L_f \cdot L_o \cdot Pd \cdot L_p \cdot \nu \qquad (1)$$

Here the mean photon number μ is set to 0.1. L_f is the loss in the transmission fiber, which is measured to be 2.3 dB/km at 850 nm for the fiber (SMF 28) used in our experiment. L_o represents other losses such as bending, coupling and connection losses in the quantum channel, which is 3 dB in our case. *Pd* is the APD's detection efficiency, about 45% (3.5 dB) at 850 nm according to the manufacturer's specification. L_p is the protocol related loss, which is 3 dB for BB84 since half of the counts are discarded in the protocol. ν denotes quantum channel transmission rate (QCTR). In our experiment we have used three values of QCTRt 156.3, 312.5 and 625.0 Mbit/s, which correspond to Alice generating one optical pulse every 8, 4 and 2 clock periods, respectively.

The measured sifted-key rate and QBER at three QCTRs for fiber lengths of 1 and 4 km are shown in Table 1. The sifted-key rate is also plotted in Fig. 3 as function of fiber length. The solid mark points represent the measured data and the lines represent the calculated data using equation 1 at OCTRs of 625, 312.5 and 256.25 Mbit/s. The measured sifted-key rate is in compliance with the calculated data. When the QCTR is 625 MHz or higher, the dead time of the APDs will influence the detection rate and therefore the sifted-key rate will be reduced. A detailed analysis is found in [15].

Table 1. Measured sifted-key rate and QBER vs. QCTRs for fiber lengths of 1 and 4 km

QCTR (Mbit/s)	625.0		312.5		156.3	
Fiber length (km)	1	4	1	4	1	4
Measured sifted-key rate (Mbit/s)	4.14	0.92	2.32	0.46	1.26	0.23
QBER (%)	3.42	3.67	2.30	3.43	2.32	2.51

QBER is another important metric for QKD systems. When the QCTR is low, the QBER is mainly due to polarization leakage or imperfect extinction ratio since dark counts are negligible in our system. As the QCTR increases, timing jitter becomes the dominating factor for the QBER. The timing jitter increases at the higher QCTR due to data-dependent jitter of the APDs and as well as that of the VCSELs. The jitter makes the histogram of the quantum bit broader than a single time detection window. The measured results show that the QBER is higher at QCTR of 625 Mbit/s than that at lower QCTRs.

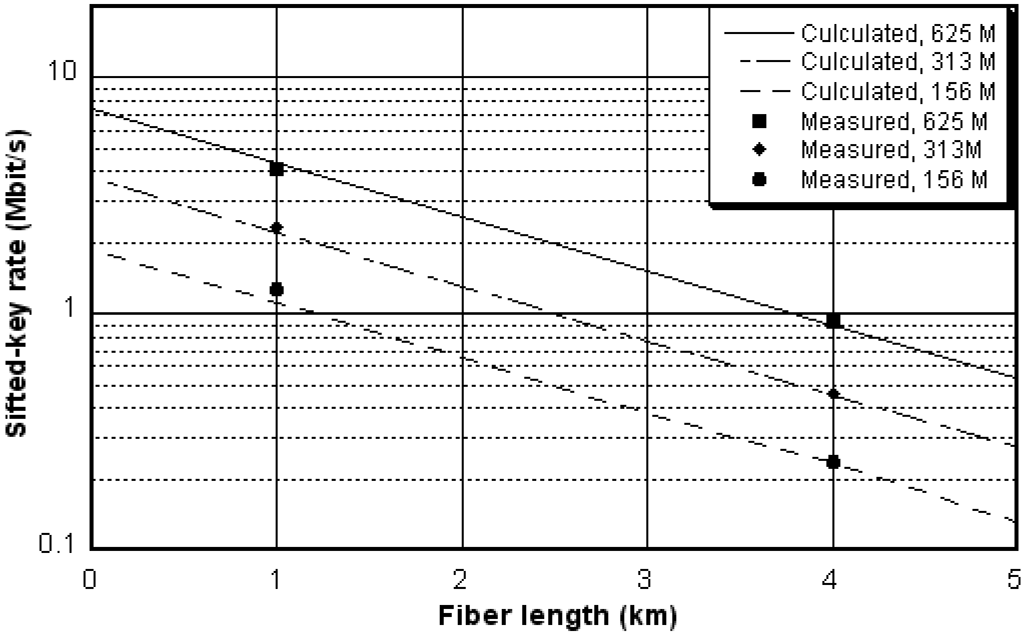

Figure 3. Sifted-key rate vs. transmission distance

4. PROPOSED SCHEMES FOR INTEGRATION INTO TELECOM INFRASTRUSTURE

The high speed QKD system presented in this paper can be integrated into a telecom infrastructure, such as a LAN, to enable secure communication and information exchange among users. From our experimental results one can see that a sifted key rate above 1 Mbit/s for fiber lengths of up to 3 km is possible. A typical campus can be equipped with such a LAN using 3 km long fibers.

In our previous demonstration [5] we used special 850nm single-mode fiber (Corning HI 780) in the quantum channel and a same length of standard telecom single-mode fiber (Corning SMF 28) for the classical channel (Fig. 4 (a)). However, the special fiber for the quantum channel is too costly for practical application.

The telecom fiber is single mode for 1550 nm but it supports two modes, the fundamental mode LP_{01} and a higher order mode LP_{11}, at 850nm. The two modes can interact and exchange energy during propagation in fiber, especially in the area of connectors, which is known as “mode coupling”. If the SMF-28 fiber is fusion spliced to a short piece (~20 cm) of HI780 fiber, which functions as a spatial filter as other groups reported [16], the higher order mode is greatly suppressed. In this work, we used a pair of standard telecom single-mode fiber for both quantum and classical channels as shown in Fig. 4 (b). Since most LANs are installed using the standard fibers in pair, this setup may be practical in many existing networks.

It is also possible to use a single fiber for both quantum and classical channels. This could make the system even more practical but one must pay a price for it. We propose two schemes for this type of QKD system. In order to use one fiber for both 850 and 1550 nm a wavelength division multiplexer (WDM) may be used to separate the two wavelengths before entering into Bob. Since WDM brings the problem of “mode coupling”, a short piece of HI 780 fiber must be used before Bob’s WDM to suppress the higher order of fiber mode generated during the transmission as shown in Fig.4(c). In this case the 1550 nm signals in the classical channel, however, is seriously reduced by the short piece if HI 780 fiber, and hence the length of the HI 780 fiber becomes very critical. It should be long enough so that the higher order mode in 850 nm is suppressed and short enough so that the reduction in 1550 nm signals do not impede normal operation.

Figure 4(d) shows another scheme that uses a single fiber for both quantum and classical channels. Here a 20/80 coupler is used. 20% of the photons are sent to Bob's classical signal receiver in the CWDM transceiver. The commercial CWDM are designed with high gain for long distance communication. With 20% of 1550 nm optical power the transceiver still works fine for classical information exchange with Alice. 80 % of the photons go through a short piece of HI 780 fiber and then enter into Bob's quantum paths. The HI780 fiber blocks 1550 nm photons and suppresses the higher order of fiber mode at 850 nm. In this scheme the resulting degradation is loss of 20% of the photons at 850 nm.

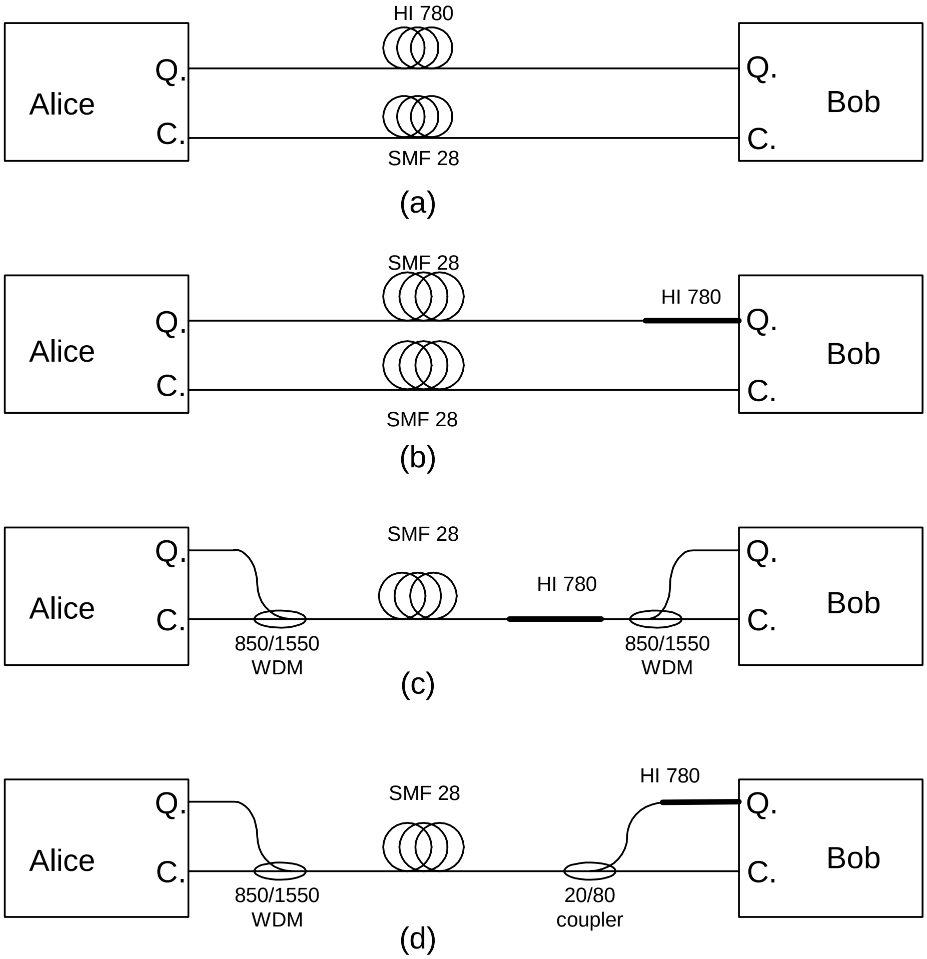

Figure 4. Four possible schemes for QKD integration into local area networks

5. CONCLUSION

We have implemented a polarization encoding fiber-based QKD system using the BB84 protocol. The system operates at a sifted key rate over 4 Mbit/s over 1 km of standard telecom fiber at a mean photon number μ = 0.1. In comparison with the previous B92 system, this system provides higher security and higher key rate. An experiment with 4 km of standard fiber was also performed. A polarization auto-compensation module and an automatic timing alignment procedure are implemented and utilized in the system, which enables the development of turn-key high-speed QKD system and its future operation in field. We also proposed four schemes for integrating the system into standard telecom infrastructure. In conclusion, QKD systems of this type appear to be very promising for practical application in secured networks.

ACKNOWLEDGEMENT

This work was supported in part by the Defense Advanced Research Projects Agency under the DARPA QuIST program.

REFERENCES

1. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing” in Proc. of the IEEE Int. Conf. on Computers, Systems & Signal Processing, pp. 175-179, Bangalore, India, December 10-12, (1984).
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography” Rev. Mod. Phys. Vol. 74, 145~195 (2002).
3. J. C. Bienfang, A. J. Gross, A. Mink, et al. “Quantum key distribution with 1.25 Gbps clock synchronization”, Optics Express. Vol. 7 (9), 2011 (2004).
4. J. G. Rarity, P. R. Tapster and P. M. Gorman, “ Secure Free-space key-exchange to 1.9 km and beyond”, Journal of Modern Optics, vol. 48, 1887-1901 (2001).
5. X. Tang, L. Ma, A. Mink, A. Nakassis, B. Hershman, J. Bienfang, R. F. Boisvert, C. Clark, and C. Williams, “High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding,” in Optics and Photonics 2005: Quantum Communications and Quantum Imaging III, Proc. SPIE 5893, 1A-1-1A-9 (2005)
6. C. Gobby, Z. L. Yuan, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber”, Applied Physics Letters, Vol. 84, 3762-3764 (2004).
7. D. S. Bethune, M. Navarro and W. P. Risk “Enhanced autocompensating quantum cryptography system”, Applied Optics, Vol. 41, 1640-1648 (2002).
8. J. Breguet, A. Muller and N. Gisin, “Quantum cryptography with polarized photons in optical fibers, experiment and practical limits”, Journal of Modern Optics, vol. 41, 2405-2412 (1994).
9. K.J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller, “A Short Wavelength GigaHertz Clocked Fiber-Optic Quantum Key Distribution System”, IEEE J. of Quantum Electronics, Vol. 40, 900-908 (2004).
10. C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Phys. Rev. Lett., 68, 3121-3124 (1992).
11. A. Mink, X. Tang, L. Ma, A. Nakassis, B. Hershman, J. Bienfang, D. Su, R. F. Boisvert, C. Clark, and C. Williams, “High Speed Quantum Key Distribution System Supports One-Time Pad Encryption of Real-Time Video”, Proc. of SPIE Quantum Information and Computation IV, Orlando, FL, 17-21 Apr 2006.
12. A. Nakassis, J. Bienfang, and C. Williams, “Expeditious reconciliation for practical quantum key distribution,” in Defense and Security Symposium: Quantum Information and Computation II, Proc. SPIE 5436, 28-35 (2004)
13. B. Huttner, A.Muller, J.D. Gautier, H. Zbinden, and N.Gisin, “ Unambiguous quantum measurement of nonorthogonal states” Physical Review A, Vol 54(5), 3783~2788 (1996)
14. Meadowlark optics catalog: liquid crystals section, http://www.meadowlark.com/catalog/LiquidCrystals.pdf
15. X. Tang, L. Ma, A. Mink, A. Nakassis, B. Hershman, J. Bienfang, D. Su, R. F. Boisvert, C. Clark, and C. Williams, “Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s”, Optics Express. Vol. 14(6), 2062-2070 (2006).
16. Paul D. Townsend, “Experimental Investigation of the Performance Limits for First Telecommunications-window Quantum cryptography Systems”, IEEE Photonics Technology Letters, Vol. 10, No.7, 1048-1050 (1998).